Background

Local Administrator Password Solution (LAPS) is a great AD feature that in a secure way mange local administrator passwords. It offers a way to prevent the reuse one the same password on multiple machines. LAPS sets a complex and unique password for every computer in the domain. Thus removing the possibility for lateral movement once a local admin password has been found. Before LAPS local administrator passwords were often managed through Group Policy Preferences, which was a terrible solution (as can be seen in the chapter on GPP). They were sometimes set using scripts found in the SYSVOL, again exposing them to everyone with access to the SYSVOL. Another common options was to use third party products, Thycotic, CyberArk, Liberman, etc.

To use LAPS the administrator must install LAPS on the management server. This will extend the AD schema and add two new attributes: `ms-McsAdmPwd` and `ms-Mcs-AdmPwdExpirationTime`.

`ms-McsAdmPwd` contains the local administrator password in cleartext.
`ms-Mcs-AdmPwdExpirationTime` contains the time and date when the password expires.

A LAPS agent will need to be running on each computer. It is this agent that changes the password.

If the access control of the attribute is incorrectly configured it can allow too many users to have read access to the password attribute, thus allowing a user to read the local administrator password of multiple computers.

Even if your user is not allowed to read the password it is still possible to enumerate who can read the password. Thos users are then attrctive targets.

Normally not even the computer itself should have read-access to the attributes. Only be able to update those attributes, but not read them.

How to check for existence of LAPS

To check if LAPS is running on your computer you can check for the following dll `AdmPwd.dll`, in its default location `C:\Program Files\LAPS\CSE\`.

You can check if the schema has been updated with the new attributes: `Get-ADObject 'CN=ms-mcs-admpwd, CN=Schema, CN=configuration, DC=evilcorp, DC=local'` If it returns data it has the updated schema, otherwise you will get an error.

The attribute `ms-Mcs-AdmPwdExpirationTime` is readible to everyone. So every computer that is administrated using LAPS will have this attribute. It is therefore possible to enumerate all computers that are nog included in LAPS.

Using the PowerSploit command `get-DomainGpo -Identity "*LAPS*"`.

I haven't tested this one. But it should list

```
Get-NetOU |
    Get-ObjectAcl -ResolveGUIDs |
    Where-Object {
        ($_.ObjectType -like 'ms-Mcs-AdmPwd') -and
        ($_.ActiveDirectoryRights -match 'ReadProperty')
    } | ForEach-Object {
        $_ | Add-Member NoteProperty 'IdentitySID' $(Convert-NameToSid $_.IdentityReference).SID;
        $_
    }
```

Using bloodhound this query can be used:

```
MATCH (u) -[:ReadLAPSPassword]-(c:Computer) return u;
```

How to check who can view the passwords in cleartext

`Get-NetOU -FullData |`

References

https://rastamouse.me/2018/03/laps---part-1/